CALENDRIER DE MISE EN ŒUVRE DU RIA

Rédaction : Alain Dubost – MICHELIN

Coordination : Thomas Van Den Heuvel – AGENCE DE LA BIOMEDECINE

Le règlement européen sur l'IA (RIA ou AI Act) est entré en vigueur le 1er août 2024 et déploie ses dispositions progressivement sur une période de 6 à 36 mois. Il s'accompagne d'obligations qui dépendent du rôle des entreprises et des organismes publics ou privés assujettis au RIA, que nous appellerons de manière indifférenciée «entités».

Ce document n'a pas l'ambition d'être une synthèse exhaustive à valeur juridique, mais plutôt un guide pratique donnant les grandes lignes des étapes menant à la conformité. La consultation et la validation par un service juridique habilité sont nécessaires pour chaque entité concernée, dans son propre contexte d'usage et d'activités.

Pour commencer, nous considérerons les obligations s'imposant à chaque entité en fonction de leur rôle et de la nature des systèmes d'IA, ainsi que de leur niveau de risque. Nous listerons ensuite les étapes clefs et leur positionnement calendaire, en émettant quelques recommandations pratiques, afin d'aider ces entités à se mettre en conformité. Enfin, nous conclurons en listant des approches complémentaires ou similaires.

En annexe, une synthèse chronologique simplifiée permet une lecture guidée visuelle de ce document.

Ce document n'aborde pas la question de la gouvernance européenne et nationale pour l'implémentation et la supervision du RIA. Par ailleurs, nous abordons essentiellement le point de vue des entreprises et des organismes publics ou privés assujettis au RIA et ne nous attardons pas sur les spécificités propres aux autorités publiques, pour lesquelles des échéances supplémentaires, des cas d'usage et des exceptions spécifiques existent concernant la mise en conformité de certains types de traitements. Enfin, les concepts ne sont pas tous définis ici, nous renvoyons pour cela le lecteur au RIA[1] ou aux fiches et aux FAQ ad hoc produites par le Clusif et l'AFCDP.

OBLIGATIONS

> NATURE DU SIA

Deux natures différentes de systèmes d'IA sont à considérer :

➜ "Système d'IA» : système automatisé conçu pour fonctionner à différents niveaux d'autonomie et pouvant faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer différentes sorties, telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels.

➜ «Modèle d'IA à usage général» : modèle d'IA qui, y compris lorsqu'il est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, présente une grande généralité et est capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché. Le modèle d'IA à usage général peut être intégré dans une variété de systèmes ou d'applications, en aval.

[1] Texte officiel du RIA : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1689

> NIVEAU DE RISQUE

Le RIA propose une approche fondée sur les risques, en classant les systèmes d'IA en quatre niveaux[2] : Risque inacceptable, Haut risque (ou risque élevé), Risque limité en matière de transparence, Risque minimal.

> RÔLE DE L'ENTITÉ

Du point de vue de l'entité assujettie, les deux rôles principaux du RIA à considérer ici sont :

➜ «Fournisseur» (ou provider) : personne physique ou morale qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit. Cela couvre le cas de l'entité qui crée un SIA en propre pour un usage interne ;

➜ «Déployeur» (ou deployer) : personne physique ou morale utilisant sous sa propre autorité un système d'IA, sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel. Un fournisseur peut ainsi également avoir le rôle de déployeur.

À noter qu'un déployeur peut devenir fournisseur lorsqu'il utilise un produit fourni par un tiers et y apporte des modifications «substantielles», ce qui peut inclure, sans s'y limiter, des modifications :

➜ Non prévues ou non planifiées par le fournisseur ;
➜ Ne faisant pas suite à une mise à jour logicielle majeure d'un système du fournisseur
➜ Pouvant remettre en cause la classification du niveau de risque ou sa conformité (haut risque ou prohibé) ;
➜ Modifiant ou faisant évoluer sa destination ;
➜ De réentraînement, d'ajustement du modèle, ou d'apprentissage par transfert de données personnelles.

SYNTHÈSE

Pour les «systèmes d'IA», le tableau suivant résume les obligations principales qui s'imposent en fonction du rôle de l'entité et du niveau de risque.

Niveau de risque	Fournisseur	Déployeur
Inacceptable	Prohibé	Prohibé
Haut (ou élevé)	Gestion des risques Gouvernance des données, qualité et sécurité Documentation technique Information et transparence Conformité et enregistrement Surveillance et mise à jour	Gouvernance des données, qualité et sécurité Contrôle humain Information et transparence Analyse d'impact (si nécessaire)
Limité	Information et transparence	Information et transparence
Minime	Code de conduite	Code de conduite

DATES CLÉS

Le premier août 2024 est la date d'entrée en vigueur de la loi sur l'IA. À cette date, aucune des exigences de la loi ne s'applique (elles entrent en vigueur progressivement). Cette mise en œuvre progressive se fait en quatre étapes principales dans le contexte de l'entité assujettie au RIA, nous les détaillons dans la suite de ce chapitre.[3]

[2] Nous ne détaillons pas ces niveaux ici, ils sont décrits dans le RIA et seront développés dans la fiche « Introduction au RIA » produite par le Clusif et l'AFCDP
[3] Pour plus de détails sur les dates clefs, les obligations et les livrables des régulateurs de l'UE : https://artificialintelligenceact.eu/implementation-timeline/

2 FÉVRIER 2025 : SYSTÈMES D'IA PROHIBÉS ET SENSIBILISATION

Obligations

Depuis cette date, les interdictions relatives à certains systèmes d'IA et les exigences en matière de sensibilisation des utilisateurs à l'IA s'appliquent.

Recommandations

> GLOBALES

De manière globale, les actions suivantes sont recommandées :

➜ Créer ou adapter une charte éthique ;

➜ Créer ou adapter une gouvernance afin de définir les principes d'utilisation de l'IA et d'assurer leur respect en accord avec les valeurs de l'entité, la stratégie business et les exigences du RIA ;

➜ Définir les rôles et responsabilités (RACI) associées pour la mise en œuvre opérationnelle dans chaque Direction, incluant également le contrôle interne.

> SYSTÈMES PROHIBÉS

Pour ce volet concernant les systèmes d'IA prohibés, l'approche suivante peut être prise :

➜ Créer un inventaire des cas d'usage et systèmes d'IA (existants et processus de mise à jour continue), en considérant également les composantes IA intégrées à d'autres solutions ;

➜ Catégoriser chacun de ces cas d'usage et systèmes d'IA selon leur niveau de risque (inacceptable, haut risque, limité ou minimal), si besoin en se faisant assister par un expert juridique ou métier ;

➜ Déterminer la nature de l'IA utilisée (système ou modèle général) ;

➜ Identifier le rôle de l'entité (fournisseur ou déployeur) ;

➜ En déduire les obligations légales applicables.

Cet inventaire sera réalisé avec l'ensemble des Directions et devra être le plus large possible, afin d'identifier les cas d'usage et systèmes d'IA existants et de détecter d'éventuels cas prohibés. Le cas échéant, un plan d'action correctif devra être mis en place rapidement, et consistera en général : soit en l'abandon du cas d'usage ou système d'IA en cause, soit en une réduction importante de sa finalité ou de son périmètre. Une attention particulière sera portée aux cas d'usage et systèmes d'IA liés aux processus de gestion des Ressources humaines (RH), ceux-ci étant les plus susceptibles de présenter les risques les plus élevés dans le contexte de l'entité (non-discrimination, protection de la vie privée…)

Par ailleurs, une actualisation continue doit être mise en place, par exemple dans le processus de gouvernance des projets. Celle-ci doit impliquer toutes les Directions et pourra se baser sur un formulaire d'auto-évaluation afin d'identifier notamment les cas d'usage ou systèmes d'IA potentiels à risque inacceptable ou à haut risque, que ce soit pour la conception, le déploiement ou l'utilisation.

> SENSIBILISATION

Pour ce volet concernant la sensibilisation, on considérera :

➜ Une sensibilisation générale de tous les employés susceptibles d'être exposés à des systèmes d'IA, qu'ils soient utilisateurs potentiels ou simplement impactés (enjeux, bénéfices, risques, limites) ;

➜ Des formations plus ciblées sur les populations mettant en œuvre ces technologies (développeurs, intégrateurs…) ou les utilisant de manière régulière dans leur activité professionnelle (risques particuliers, par exemple : propriété intellectuelle, protection des données personnelles, biais…).

2 AOÛT 2025 : MODÈLES D'IA À USAGE GÉNÉRAL

> OBLIGATIONS

À cette date, les dispositions du RIA relatives aux modèles d'IA à usage général (ou GPAI) s'appliquent. La gouvernance au niveau des autorités est également en place, incluant les organismes notifiés, le respect de la confidentialité et les sanctions applicables.
À noter que les fournisseurs de modèles GPAI qui ont été mis sur le marché ou mis en service avant cette date doivent se conformer au RIA avant le 2 août 2027.
Les modèles GPAI doivent se conformer à des exigences afin de cadrer leur usag e :

- ➜ Fournir une documentation technique ;
- ➜ Mettre en oeuvre des politiques de conformité au droit de propriété intellectuelle (et copyright) ;
- ➜ Fournir une information détaillée concernant les jeux de données d'apprentissage ;
- ➜ Être en mesure de démontrer la conformité.

Dans le cas où il existerait des risques systémiques, des obligations complémentaires s'appliquent :

- ➜ Évaluation et maîtrise des risques ;
- ➜ Suivi et notification des incidents aux autorités ;
- ➜ Mise en oeuvre de mesures de cybersécurité adaptées.

Un risque systémique est défini comme « tout effet négatif réel ou raisonnablement prévisible en rapport avec des accidents majeurs, des perturbations de secteurs critiques et des conséquences graves pour la santé et la sécurité publiques, tout effet négatif réel ou raisonnablement prévisible sur les processus démocratiques, la sécurité publique et la sécurité économique, et la diffusion de contenus illicites, faux ou discriminatoires[4] ».

> RECOMMANDATIONS

Concernant les modèles GPAI, les obligations incombent en majeure partie aux fournisseurs. Elles concernent également les déployeurs, notamment dans le cas d'utilisation de modèles qui sont entraînés en interne à l'entité. Dans tous les cas, la documentation et la conformité doivent être prises en compte lors de la mise à disposition de ces outils aux utilisateurs.
Pour les entités couvertes par la présente fiche, le risque systémique associé à l'utilisation d'un modèle GPAI devrait être peu courant, selon son secteur d'activité. Néanmoins, nous recommandons que ces usages fassent partie de l'inventaire des cas d'usage et systèmes d'IA mentionné au chapitre précédent, afin d'analyser l'éventuelle présence d'un tel risque. Le cas échéant, il faudra mettre en place une maîtrise des risques adaptée, un processus de suivi et de notification des incidents, et des mesures de cybersécurité adaptées au risque (pour ces points, des codes de bonnes pratiques ont été publiés le 10 juillet 2025 par la Commission européenne et portent sur trois thèmes : sûreté et sécurité, transparence, droit d'auteur[5]).

[4] Cette définition peut être retrouvée dans le texte du RIA : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1689#rct_110

[5] Ce code de bonnes pratiques peut être consulté à l'adresse suivante : https://digital-strategy.ec.europa.eu/fr/policies/contents-code-gpai

2 AOÛT 2026 : APPLICATION GÉNÉRALE (SAUF EXCEPTION)

> OBLIGATIONS

À cette date, l'ensemble des dispositions du RIA s'applique, à l'exception des produits ou composants
de produits couverts par la législation d'harmonisation de l'Union.
Par ailleurs, les systèmes d'IA à haut risque (autres que les systèmes visés à l'article 111, paragraphe 1) mis sur le marché ou mis en service avant cette date seront concernés par cette échéance uniquement si leur conception est modifiée de manière significative à partir de cette date.

> RECOMMANDATIONS : SYSTÈMES D'IA À HAUT RISQUE

Ci-après les principaux éléments pour se mettre en conformité pour les systèmes d'IA à haut risque.

Gestion des risques - fournisseurs (et déployeurs pour analyse d'impact)

➜ Établir des processus clairs et documentés pour identifier, analyser, estimer et évaluer les risques associés aux systèmes d'IA à haut risque, vis-à-vis des déployeurs et des personnes impactées.
Ces processus doivent couvrir l'ensemble du cycle de vie des systèmes et être intégrés à la gestion globale des risques et des projets ;
➜ Déployeurs : le cas échéant, et pour les seules entités concernées, réaliser une analyse d'impact sur les droits fondamentaux et libertés des personnes (analyse HRIA et/ou AIPD pour le RGPD) ;
➜ Mettre en oeuvre les mesures d'atténuation appropriées, en fonction de la gravité et de l'occurrence
de chaque risque, et de l'état de l'art en matière de sécurité et d'éthique.

Gouvernance des données, qualité et sécurité - fournisseurs et déployeurs

➜ Nommer un responsable de la gouvernance des données dans le contexte du RIA ;
➜ Nommer un Digital Ethics Officer et définir les rôles, responsabilités et interactions respectifs ;
➜ Définir des politiques claires pour la collecte, le traitement, le stockage, la sécurisation et la suppression des données utilisées par les systèmes d'IA, conformes au RGPD (et, si possible, s'appuyant sur celles existantes) ;
➜ S'assurer qu'il existe au sein des Directions et/ou des projets un processus rigoureux pour garantir la qualité, la pertinence, la représentativité et l'absence de biais des données utilisées pour l'entraînement, la validation et le test des systèmes d'IA à haut risque ;
➜ Définir les mesures de sécurité techniques, organisationnelles et contractuelles appropriées afin de protéger les données contre les accès non autorisés, les fuites, les altérations et les destructions, conformément au RGPD et aux exigences de cybersécurité du RIA (y compris leur résilience et la traçabilité des actions), et en contrôler régulièrement l'application.

Documentation technique - fournisseurs

Pour chaque système d'IA à haut risque, rédiger une documentation technique conforme aux exigences du RIA, et définir un processus de tenue à jour, notamment lors de toute modification substantielle du système ou de son environnement d'utilisation. Celle-ci doit notamment comprendre :
➜ La description du système, de sa finalité et de son fonctionnement ;
➜ L'architecture technique et les algorithmes utilisés ;
➜ Les données d'entraînement, de validation et de test ;
➜ Les résultats des évaluations de performance et de conformité ;
➜ Les mesures de gestion des risques, de transparence et de contrôle humain ;
➜ Les instructions d'utilisation.

Contrôle humain - déployeurs

Le RIA exige que la conception des systèmes d'IA à haut risque permette un contrôle humain effectif.
➜ Pour chaque projet (cas d'usage et système d'IA), définir clairement les rôles et les responsabilités des personnes chargées du contrôle humain, en s'assurant qu'elles disposent des moyens nécessaires pour les accomplir (organisation, ressources et techniques) ;
➜ Garantir que les personnes chargées du contrôle humain disposent des compétences et de la formation nécessaires pour exercer leur rôle efficacement, avec une bonne compréhension du ystème d'IA, de ses limites et des risques associés à son utilisation ;
➜ Définir des procédures d'intervention en cas de

détection d'un risque, d'une erreur ou d'un comportement anormal du système d'IA (suspension du système, correction des données d'entrée ou modification de paramètres, par exemple).

Information et transparence - fournisseurs et déployeurs

Le RIA exige des obligations d'information à tous les stades de sa mise en oeuvre.
➜ Une information auprès des utilisateurs finaux (avec, par exemple, une bannière d'information présentée par le système d'IA, incluant les risques et limites du système, un point de contact et un lien vers une documentation détaillée) ;
➜ Le cas échéant, une consultation ou une information auprès des instances représentatives du personnel dans certains cas à haut risque ;
➜ Un moyen pour les déployeurs et les utilisateurs finaux d'obtenir l'explicabilité des décisions prises sur la base d'un système d'IA, à haut risque notamment ;
➜ Un processus de notification en cas d'incident impliquant un système d'IA (vers les personnes concernées, le fournisseur et/ou vers les autorités).

Conformité et enregistrement - fournisseurs

➜ Évaluation de la conformité du système d'IA à haut risque, pour démontrer qu'il respecte bien les exigences du RIA (selon le type, en contrôle interne ou par un organisme notifié) ;
➜ Déclaration UE de conformité et apposition du marquage CE ;
➜ Enregistrement dans la base de données de l'UE prévue à cet effet, avec une mise à jour en cas de modification substantielle.

Surveillance et mise à jour - fournisseurs

La mise en conformité avec le RIA est un processus continu dans la durée et non une action ponctuelle.
➜ Mettre en place des processus de surveillance continue des systèmes d'IA à haut risque, afin de détecter rapidement tout écart par rapport aux exigences de conformité (indicateurs, tests, audit) ;
➜ Assurer la veille juridique afin d'anticiper les évolutions et lignes directrices de la réglementation ;
➜ Intégrer le RIA dans les processus de contrôle interne et d'audit interne ;
➜ Assurer la surveillance après commercialisation, avec un processus de remontée des anomalies et des actions correctives documentées et traçables en cas de non-conformité.

> RECOMMANDATIONS : SYSTÈMES D'IA À RISQUE LIMITÉ OU MINIMAL

Information et transparence - fournisseurs et déployeurs

Pour les systèmes d'IA à risque limité, les obligations d'information et de transparence s'appliquent.
Pour les systèmes d'IA à risque minimal, la conformité est basée sur l'adhésion volontaire à un code de conduite et à des bonnes pratiques (codes de bonnes pratiques publiés le 10 juillet 2025 par la Commission européenne[6]).

[6]Ce code de bonnes pratiques peut être consulté à l'adresse suivante : https://digital-strategy.ec.europa.eu/fr/policies/contents-code-gpai

2 AOÛT 2027 : APPLICATION GÉNÉRALISÉE

> OBLIGATIONS

À cette date, l'ensemble des dispositions du RIA s'applique de manière généralisée, y compris les produits ou composants de produits couverts par la législation d'harmonisation de l'Union.
Comme énoncé précédemment, les fournisseurs de modèles GPAI mis sur le marché avant le 2 août 2025 doivent avoir pris les mesures nécessaires pour se conformer aux obligations prévues par le présent règlement avant cette date. De même, tous les systèmes d'IA à haut risque sont également concernés, en tenant compte des spécificités du RIA entre modèles open source et modèles commerciaux.
Font exception les systèmes d'IA qui sont des composants des systèmes d'information à grande échelle (Schengen, visas…[7]), mis sur le marché ou mis en service avant cette date : ceux-ci devront être en conformité avec le présent règlement avant le 31 décembre 2030. Il s'agira en général de systèmes d'IA à haut risque destinés à être utilisés par les autorités publiques [8] [9].

> RECOMMANDATIONS

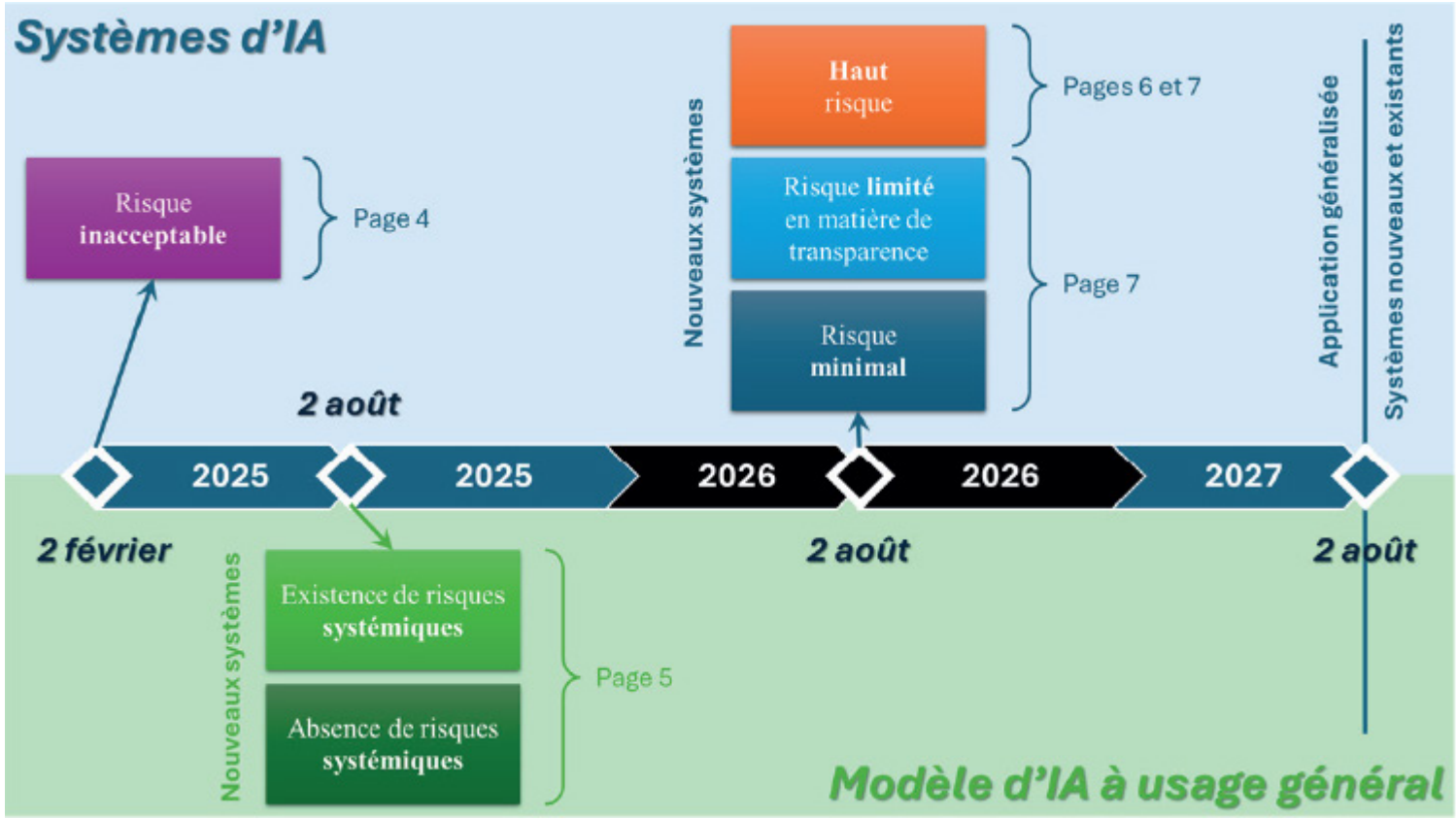
Les mêmes recommandations qu'au chapitre précédent s'appliquent sur l'ensemble du périmètre concerné et quel que soit le niveau de risque du système d'IA.

CONCLUSION

Le système de management de la qualité dans l'entité est l'une des pierres angulaires permettant de mettre en place et de démontrer sa conformité au RIA. Il est essentiel de développer une culture de l'éthique de l'IA, responsable, maîtrisant les risques, et permettant d'en tirer les bénéfices tout en respectant les droits fondamentaux des personnes.
Des travaux de certification par l'UE sont en cours et sont à suivre. Dans l'attente et à défaut, les entités recherchant un modèle pourront envisager la norme ISO/IEC 42001 (Système de management de l'intelligence artificielle), qui pourrait apporter un cadre à l'approche. Une certification vis-à-vis de cette norme pourrait également être envisagée (celle-ci n'est en rien une garantie de conformité au RIA, mais permettrait de démontrer une volonté et de donner un cadre de référence adéquat). Il existe d'autres publications utiles .
Par ailleurs, on notera quelques points communs avec le RGPD dans l'esprit et dans l'approche, notamment la structuration du niveau d'exigences par les risques. Nous encourageons les entités à capitaliser sur ce dernier et, quand cela est pertinent et possible, à mutualiser certaines responsabilités et/ou processus. À noter que les cas d'usage à haut risque impliqueront en général des données personnelles, renforçant la nécessaire synergie dans le contexte de l'entité. Il existe par ailleurs des différences (notamment le fait que le RIA ne prescrive pas un rôle de référent IA, à l'inverse du RGPD) afin que chaque entité puisse choisir son modèle adapté de gouvernance.
Un déploiement réussi sera le fruit de la collaboration des équipes business, juridiques et informatiques.

[7] Voir liste dans l'annexe X du RIA
[8] ENISA « Cybersecurity of AI and Standardisation : https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation
[9] CNIL « Fiches pratiques IA » : https://cnil.fr/fr/ia-finalisation-recommandations-developpement-des-systemes-ia

Annexe : synthèse chronologique simplifiée



Campus Cyber
5 rue Bellini
92821 Puteaux cedex
France
Tel : +33 1 53 25 08 80
clusif@clusif.fr
https://clusif.fr

1 rue de Stockholm
75008 Paris
back-office@afcdp.net
https://afcdp.net/